Math-Net.Ru

Общероссийский математический портал

В. Б. Алексеев, О некоторых алгебрах, связанных с быстрыми алгоритмами, *Дискрет. матем.*, 1996, том 8, выпуск 1, 52–64

DOI: <https://doi.org/10.4213/dm508>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.85.209

26 апреля 2023 г., 15:03:55

О некоторых алгебрах, связанных с быстрыми алгоритмами

© 1996 г. В. Б. Алексеев

В работе показано, что результаты о существовании быстрых билинейных алгоритмов для умножения комплексных чисел и кватернионов могут быть представлены просто как вложение данных алгебр в алгебры соответствующей размерности с простой таблицей умножения. Для комплексных чисел возможности такого расширения исследованы полностью.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект 94-01-01206а.

1. Введение

Одна из важных проблем современной математики — разработка алгоритмов для ускорения вычислений. Для таких алгебр, как алгебра чисел, представленных в позиционной системе, алгебра полиномов, алгебра матриц и другие, найдены алгоритмы, существенно более быстрые при больших значениях параметров, чем естественные алгоритмы. Однако, если, например, для умножения чисел и полиномов получены почти оптимальные алгоритмы, то для умножения матриц проблема далека от завершения [1].

Данная работа предлагает новый взгляд на имеющиеся результаты по построению быстрых алгебраических алгоритмов и дает новые возможности для поиска таких алгоритмов. Удастся показать, что результаты о существовании быстрых билинейных алгоритмов для умножения комплексных чисел, кватернионов и матриц порядка 2 могут быть представлены просто как вложение данных алгебр в алгебры соответствующей размерности с простой таблицей умножения. Для комплексных чисел возможности такого расширения исследованы в данной статье полностью. Все (их 3) минимальные расширения с простым умножением для алгебры матриц порядка 2 будут представлены в отдельной статье.

2. Алгебры с простым умножением

В этом параграфе мы введем в рассмотрение класс алгебр, которые оказываются непосредственно связанными с оптимальными по сложности билинейными алгоритмами умножения в некоторых известных алгебрах.

Пусть K — некоторое поле, V — векторное пространство над K с дополнительной операцией $\times$ умножения в V , удовлетворяющей свойству линейности по каждому из аргументов. Тогда V называется алгеброй над полем K .

Примерами могут служить алгебра комплексных чисел, рассматриваемая как двумерная алгебра над полем действительных чисел, или алгебра квадратных матриц порядка n над произвольным полем.

Пусть V — алгебра над полем K и $\{e_1, e_2, \dots, e_n\}$ — базис векторного пространства V . Пусть

$$e_i e_j = \sum_{k=1}^n \gamma_{ijk} e_k, \quad i = 1, \dots, n, \quad j = 1, \dots, n. \quad (1)$$

Тогда равенства (1) полностью определяют умножение в V , поскольку, с учетом линейности умножения по обоим аргументам,

$$\begin{aligned} \sum_{i=1}^n \alpha_i e_i \sum_{j=1}^n \beta_j e_j &= \sum_{i=1}^n \sum_{j=1}^n \alpha_i \beta_j (e_i e_j) \\ &= \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n \alpha_i \beta_j \gamma_{ijk} e_k = \sum_{k=1}^n \sum_{i=1}^n \sum_{j=1}^n \alpha_i \beta_j \gamma_{ijk} e_k. \end{aligned} \quad (2)$$

Набор коэффициентов γ_{ijk} называют тензором алгебры V в базисе $\{e_1, e_2, \dots, e_n\}$, а сами выражения (1) таблицей умножения в V в данном базисе.

Начнем со следующего примера. Рассмотрим алгебру C комплексных чисел как двумерную алгебру над полем действительных чисел. Взяв стандартный базис $\{1, i\}$, мы получим стандартное представление $a + bi$ комплексного числа с координатами (a, b) . Используя стандартную таблицу умножения: $1 \cdot 1 = 1$, $1 \cdot i = i \cdot 1 = i$, $i \cdot i = -1$, получаем, что

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i. \quad (3)$$

Согласно (3) вычисление координат произведения в C требует 4 умножения координат сомножителей. Известен следующий алгоритм вычисления координат произведения в (3):

$$F_1 = (a + b)(c + d), \quad F_2 = ac, \quad F_3 = bd, \quad ac - bd = F_2 - F_3, \quad ad + bc = F_1 - F_2 - F_3.$$

Этот алгоритм требует только 3 умножения, правда не самих координат сомножителей, а их линейных форм. Можно поставить вопрос: нельзя ли добиться, чтобы умножение в C выполнялось с использованием только 3 умножений самих координат сомножителей? Ясно, что в стандартном базисе $\{1, i\}$ этого сделать нельзя. Нетрудно показать, что и в любом другом базисе это невозможно. Однако, оказывается, что решение есть, но только рассматривать надо не саму алгебру C , а некоторое ее расширение.

Рассмотрим 3-мерную алгебру AC с базисом e_1, e_2, e_3 и таблицей умножения

$$\begin{aligned} e_1 e_1 &= e_1 + e_3, & e_2 e_2 &= e_2 - e_3, \\ e_3 e_3 &= -2e_1 - e_2 - e_3, & e_i e_j &= 0, \quad i \neq j. \end{aligned} \quad (4)$$

Предложение 1. Алгебра AC содержит двумерную подалгебру, изоморфную алгебре C комплексных чисел.

Доказательство. Пусть $\{1, i\}$ — стандартный базис в C . Положим $\varphi(1) = g_1 = e_1 + e_2$, $\varphi(i) = g_i = e_1 + e_3$, $\varphi(a + bi) = ag_1 + bg_i$. Очевидно, это вложение изоморфно относительно сложения элементов и умножения на действительную константу. Справедливы равенства

$$\begin{aligned} g_1 g_1 &= (e_1 + e_2)(e_1 + e_2) = e_1 e_1 + e_2 e_2 \\ &= (e_1 + e_3) + (e_2 - e_3) = e_1 + e_2 = g_1, \\ g_1 g_i &= (e_1 + e_2)(e_1 + e_3) = e_1 e_1 = e_1 + e_3 = g_i, \\ g_i g_1 &= (e_1 + e_3)(e_1 + e_2) = e_1 e_1 = e_1 + e_3 = g_i, \\ g_i g_i &= (e_1 + e_3)(e_1 + e_3) = e_1 e_1 + e_3 e_3 \\ &= (e_1 + e_3) + (-2e_1 - e_2 - e_3) = -e_1 - e_2 = -g_1, \\ \varphi(a + bi)\varphi(c + di) &= (ag_1 + bg_i)(cg_1 + dg_i) = (ac - bd)g_1 + (ad + bc)g_i \\ &= \varphi((ac - bd) + (ad + bc)i). \end{aligned}$$

Таким образом, φ — изоморфное вложение C в AC . Утверждение доказано.

Запишем таблицу умножения (4) в виде

$$e_i e_i = \sum_{k=1}^n \gamma_{ik} e_k, \quad i = 1, 2, 3.$$

Тогда

$$\sum_{i=1}^n \alpha_i e_i \sum_{j=1}^n \beta_j e_j = \sum_{k=1}^n \sum_{i=1}^n \alpha_i \beta_i \gamma_{ik} e_k. \quad (5)$$

Так как γ_{ik} — фиксированные константы, вычисление произведения в AC в выбранном базисе требует только трех умножений координат сомножителей.

Доказанное утверждение может иметь следующее практическое применение. Если необходимо производить большие вычисления с комплексными числами, то можно хранить их не в стандартном базисе, а в виде их образов в алгебре AC в базисе e_1, e_2, e_3 , не возвращаясь после каждой операции в стандартную форму. Операции сложения и умножения на действительное число будут выполняться покомпонентно, а умножение потребует только трех умножений компонент чисел, а также одного умножения на 2 и четырех сложений и вычитаний. Число сложений и вычитаний можно свести до трех, если заметить, что коэффициенты при e_1 и e_2 в правой части в (5) вычисляются по формулам $\alpha_1 \beta_1 - 2\alpha_3 \beta_3$ и $\alpha_2 \beta_2 - \alpha_3 \beta_3$, а коэффициент при e_3 равен разности этих выражений. Следует заметить, однако, что память для хранения комплексных чисел при таком подходе увеличивается в полтора раза.

С теоретической точки зрения приведенная алгебра AC интересна как расширение алгебры комплексных чисел, обладающее определенными хорошими свойствами (простым умножением). Правда так же, как при переходе от комплексных чисел к кватернионам, здесь теряются некоторые свойства. Если при переходе к кватернионам теряется коммутативность, то при переходе к AC коммутативность сохраняется, но появляются делители нуля и пропадает ассоциативность: $e_1(e_1 e_3) = 0$, но $(e_1 e_1)e_3 = e_3 e_3 \neq 0$.

Естественно возникает вопрос: насколько приведенный пример уникален? Во-первых, существуют ли другие трехмерные алгебры с простым умножением, являющиеся расширением поля комплексных чисел? Во-вторых, для умножения в ряде алгебр известны алгоритмы с меньшим, чем в стандартных алгоритмах, числом умножений линейных форм от коэффициентов. Так, для умножения кватернионов над полем действительных чисел существует алгоритм с 8 умножениями вместо обычных 16, для умножения квадратных матриц порядка 2 существует алгоритм с 7 умножениями вместо обычных 8. Спрашивается, связано ли это с существованием для них расширений соответствующей размерности с простым умножением?

Прежде, чем ответить на эти вопросы, необходимо дать строгое определение тех алгебр, которые могут рассматриваться в качестве искомым расширений. Если, обобщая приведенный выше пример, рассматривать только алгебры с условием $e_i e_j = 0$ при $i \neq j$, то все такие алгебры будут коммутативны и, следовательно, не могут быть расширением, например, алгебры матриц. Поэтому мы введем в рассмотрение более общий класс алгебр следующим образом.

Пусть V — алгебра на поле K . Тогда V будет называться алгеброй с простым умножением, если существует такой базис $e_1, e_2, \dots, e_n$ в V и такая подстановка σ на множестве $\{1, 2, \dots, n\}$, что $e_i e_j = 0$ при $j \neq \sigma(i)$.

Таким образом, умножение в n -мерной алгебре V с простым умножением задается n равенствами

$$e_i e_{\sigma(i)} = f_i = \sum_{k=1}^n \gamma_{ik} e_k, \quad i = 1, 2, \dots, n, \quad (6)$$

и условием, что все остальные произведения базисных векторов равны 0.

Пусть V — алгебра над некоторым полем K . Через $\dim_A V$ будем обозначать наименьшую размерность алгебры с простым умножением над полем K , содержащей подалгебру, изоморфную V .

Рассмотрим связь $\dim_A V$ с билинейной сложностью, которая определяется следующим образом. Пусть произведение в алгебре V над полем K задается равенствами (1) и (2). Положим

$$\delta_k = \sum_{i=1}^n \sum_{j=1}^n \alpha_i \beta_j \gamma_{ijk}, \quad k = 1, 2, \dots, n. \quad (7)$$

Последовательность выражений

$$F_m = F'_m F''_m, \quad m = 1, 2, \dots, r, \quad p_k = \sum_{m=1}^r c_{km} F_m, \quad k = 1, 2, \dots, n, \quad (8)$$

где F'_m — линейные формы с коэффициентами из поля K от переменных α_i , F''_m — линейные формы с коэффициентами из K от переменных β_j , $c_{km} \in K$ и $p_k = \delta_k$ при всех k , называется билинейным алгоритмом сложности r для вычисления произведения в алгебре V в базисе $e_1, e_2, \dots, e_n$. Билинейной сложностью умножения в алгебре V называется минимальная сложность билинейного алгоритма для вычисления произведения в этой алгебре. Нетрудно видеть, что билинейная сложность умножения в алгебре V над полем K не зависит от выбора базиса в V , что вытекает из следующей леммы.

Лемма 1. Если для вычисления произведения в алгебре V существует билинейный алгоритм сложности r в одном базисе, то существует билинейный алгоритм сложности r и в любом другом базисе.

Доказательство. Пусть $\alpha_i, \beta_j, \delta_k$ — координаты перемножаемых векторов и произведения в первом базисе, а $\alpha'_i, \beta'_j, \delta'_k$ — их координаты во втором базисе, и пусть билинейный алгоритм для вычисления произведения в первом базисе задается равенствами (8). Так как δ'_k — фиксированные линейные комбинации координат δ_k , то δ'_k можно выразить как линейные комбинации тех же билинейных форм F_m от перемножаемых векторов. Поскольку F'_m, F''_m — линейные формы, соответственно, от α_i и β_j , α_i — линейные формы от α'_i, β_j — линейные формы от β'_j , то F'_m, F''_m можно записать в виде линейных форм, соответственно, от α'_i и β'_j . Получим билинейный алгоритм сложности r во втором базисе. Лемма доказана.

Будем обозначать билинейную сложность умножения в алгебре V через $L_b(V)$.

Лемма 2. Пусть алгебра V_1 содержит подалгебру V_2 . Тогда $L_b(V_1) \geq L_b(V_2)$.

Доказательство. Пусть $e_1, \dots, e_q$ — базис в V_2 . Тогда его можно дополнить до базиса $e_1, \dots, e_q, e_{q+1}, \dots, e_n$ в V_1 . Пусть билинейная сложность умножения в V_1 равна r . Тогда по лемме 1 для умножения в V_1 существует билинейный алгоритм сложности r в базисе $e_1, \dots, e_q, e_{q+1}, \dots, e_n$. Положив в этом алгоритме $\alpha_i = 0, \beta_j = 0$ для всех $i > q, j > q$, получим билинейный алгоритм сложности r для умножения в V_2 . Лемма доказана.

Лемма 3. Пусть V_1 — алгебра с простым умножением, содержащая подалгебру, изоморфную алгебре V_2 . Тогда размерность алгебры V_1 не меньше, чем билинейная сложность умножения в алгебре V_2 .

Доказательство. Пусть $\dim V_1 = n$ и таблица умножения в V_1 задается равенствами (6). Тогда из (7) получаем, что

$$\delta_k = \sum_{i=1}^n \alpha_i \beta_{\sigma(i)} \gamma_{ik}, \quad k = 1, 2, \dots, n.$$

Пусть

$$F_i = \alpha_i \beta_{\sigma(i)}, \quad i = 1, \dots, n, \quad p_k = \sum_{i=1}^n \gamma_{ik} F_i, \quad k = 1, \dots, n.$$

Мы получаем билинейный алгоритм для умножения в V_1 сложности n . Следовательно, билинейная сложность умножения в V_1 не больше n , и по лемме 2 билинейная сложность умножения в V_2 также не больше n . Лемма доказана.

Лемма 3 утверждает, что $\dim_A V \geq L_b(V)$. Можно предположить, что в этой оценке всегда справедливо равенство. Приводимый ниже пример показывает, что это не так.

Предложение 2. Существует алгебра V такая, что $L_b(V) = 2$ и $\dim_A V \geq 3$.

Доказательство. Пусть V — двумерная алгебра над полем действительных чисел со следующей операцией умножения в некотором базисе e_1, e_2 :

$$(\alpha_1 e_1 + \alpha_2 e_2)(\beta_1 e_1 + \beta_2 e_2) = \alpha_1 \beta_1 e_1 + (\alpha_1 + \alpha_2)(\beta_1 - \beta_2) e_2 \quad (9)$$

Заметим, что эта операция некоммутативна. Пусть $F'_1 = \alpha_1$, $F''_1 = \beta_1$, $F'_2 = \alpha_1 + \alpha_2$, $F''_2 = \beta_1 - \beta_2$. Тогда $\alpha_1 \beta_1 = F'_1 F''_1$, $(\alpha_1 + \alpha_2)(\beta_1 - \beta_2) = F'_2 F''_2$, откуда получаем, что $L_b(V) \leq 2$. Поскольку билинейные формы при e_1 и e_2 в правой части в (9) линейно независимы, то $L_b(V) = 2$. Допустим, что существует двумерная алгебра V_1 с простым умножением, содержащая подалгебру V . Так как в этом случае $\dim V_1 = \dim V = 2$, то V_1 совпадает с V , то есть V должна быть алгеброй с простым умножением. Пусть $h = ae_1 + be_2$ и $hh = 0$ в алгебре V . Тогда $a^2 e_1 + (a+b)(a-b)e_2 = 0$. Отсюда, $a = 0$, $b = 0$, то есть $h = 0$. Следовательно, если $h \neq 0$, то $hh \neq 0$. Допустим, что e_1, e_2 — базис в V , в котором таблица умножения является простой. Тогда $e_1 e_1 \neq 0$, $e_2 e_2 \neq 0$ и, следовательно, $e_1 e_2 = e_2 e_1 = 0$. Но тогда операция умножения в V оказывается коммутативной, и мы получаем противоречие. Утверждение доказано.

Таким образом, не обязательно $\dim_A V = L_b(V)$. В общем случае мы можем лишь утверждать, что $\dim_A V \leq 2L_b(V)$, хотя в некоторых важных частных случаях оказывается, что $\dim_A V = L_b(V)$. Так предложение 1 показывает, что такова ситуация для алгебры комплексных чисел над полем действительных чисел, поскольку известно, что билинейная сложность этой алгебры равна 3.

Следующая теорема показывает, что аналогичная ситуация имеет место и для алгебры кватернионов над полем действительных чисел. Напомним, что кватернионы — это 4-мерная алгебра над полем действительных чисел, таблица умножения в которой в стандартном базисе $\{1, i, j, k\}$ задается равенствами: для любого x

$$\begin{aligned} 1 \cdot x = x \cdot 1 = x, \quad i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \\ ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j. \end{aligned} \quad (10)$$

Известно, что билинейная сложность умножения кватернионов над полем действительных чисел равна 8 [2].

Теорема 1. Существует 8-мерная алгебра с простым умножением над полем действительных чисел, являющаяся расширением алгебры кватернионов.

Доказательство. Пусть AQ — это 8-мерная алгебра с простым умножением над полем действительных чисел, умножение в которой выполняется в соответствии с таблицей 1 (например: $e_1 e_1 = f_1 = -2e_1 + e_2 + e_3 + e_4 + e_5$). Пусть $\{1, i, j, k\}$ — стандартный базис в алгебре кватернионов. Положим

$$\begin{aligned} \varphi(1) = g_1 = -e_1 + \frac{1}{2}e_2 + \frac{1}{2}e_3 + \frac{1}{2}e_4 + \frac{1}{2}e_5, \\ \varphi(i) = g_i = -\frac{1}{2}e_2 - \frac{1}{2}e_3 + \frac{1}{2}e_4 + \frac{1}{2}e_5 + e_6, \end{aligned}$$

Таблица 1.

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
$e_1 e_1 = f_1$	-2	1	1	1	1	0	0	0
$e_2 e_2 = f_2$	1	1	-1	-1	-1	-1	-1	-1
$e_3 e_3 = f_3$	1	-1	1	-1	-1	-1	1	1
$e_4 e_4 = f_4$	1	-1	-1	1	-1	1	-1	1
$e_5 e_5 = f_5$	1	-1	-1	-1	1	1	1	-1
$e_7 e_8 = f_6$	0	-1	-1	1	1	2	0	0
$e_8 e_6 = f_7$	0	-1	1	-1	1	0	2	0
$e_6 e_7 = f_8$	0	-1	1	1	-1	0	0	2

$$\varphi(j) = g_j = -\frac{1}{2}e_2 + \frac{1}{2}e_3 - \frac{1}{2}e_4 + \frac{1}{2}e_5 + e_7,$$

$$\varphi(k) = g_k = -\frac{1}{2}e_2 + \frac{1}{2}e_3 + \frac{1}{2}e_4 - \frac{1}{2}e_5 + e_8,$$

$$\varphi(a + bi + cj + dk) = ag_1 + bg_i + cg_j + dg_k.$$

Тогда φ — взаимно однозначное вложение кватернионов в AQ , изоморфное относительно сложения и умножения на действительную константу. Кроме того,

$$g_1 g_1 = f_1 + \frac{1}{4}f_2 + \frac{1}{4}f_3 + \frac{1}{4}f_4 + \frac{1}{4}f_5 = g_1,$$

$$g_1 g_i = g_i g_1 = -\frac{1}{4}f_2 - \frac{1}{4}f_3 + \frac{1}{4}f_4 + \frac{1}{4}f_5 = g_i,$$

$$g_i g_i = \frac{1}{4}f_2 + \frac{1}{4}f_3 + \frac{1}{4}f_4 + \frac{1}{4}f_5 = -g_1,$$

$$g_i g_j = \frac{1}{4}f_2 - \frac{1}{4}f_3 - \frac{1}{4}f_4 + \frac{1}{4}f_5 + f_8 = g_k,$$

$$g_i g_k = \frac{1}{4}f_2 - \frac{1}{4}f_3 + \frac{1}{4}f_4 - \frac{1}{4}f_5 = -g_j.$$

Легко видеть, что линейное отображение ψ алгебры AQ на себя, такое, что $\psi(e_i) = e_i$ при $i = 1, \dots, 5$ и $\psi(e_6) = e_7$, $\psi(e_7) = e_8$, $\psi(e_8) = e_6$, является автоморфизмом алгебры AQ . При этом $\psi(g_1) = g_1$, $\psi(g_i) = g_j$, $\psi(g_j) = g_k$, $\psi(g_k) = g_i$. Поэтому для g_1, g_i, g_j, g_k справедливы все тождества, аналогичные тождествам (10), то есть порожденная ими подалгебра в AQ изоморфна алгебре кватернионов. Теорема доказана.

3. Минимальные расширения с простым умножением для алгебры комплексных чисел

Известно, что билинейная сложность умножения комплексных чисел над полем действительных чисел равна 3, то есть сама двумерная алгебра комплексных

чисел не является алгеброй с простым умножением. Здесь мы докажем следующую теорему.

Теорема 2. Все (с точностью до изоморфизма) трехмерные алгебры с простым умножением над полем действительных чисел, являющиеся расширением алгебры комплексных чисел, — это алгебры следующих четырех типов: алгебры типа AC1, для которых

$$\begin{aligned} e_1 e_1 &= e_1 + e_3, \\ e_2 e_2 &= e_2 - e_3, \\ e_3 e_3 &= -\frac{1}{(b-a)^2}((1+a^2)e_1 + (1+b^2)e_2 + (a^2-b^2)e_3), \quad a \neq b; \end{aligned}$$

алгебры типа AC2, для которых

$$\begin{aligned} e_1 e_1 &= e_1 + \frac{F}{(c-a)(a-b)}, \\ e_2 e_2 &= e_2 + \frac{F}{(a-b)(b-c)}, \\ e_3 e_3 &= e_3 + \frac{F}{(b-c)(c-a)}, \quad a \neq b, \quad a \neq c, \quad b \neq c, \\ F &= (a^2+1)e_1 + (b^2+1)e_2 + (c^2+1)e_3; \end{aligned}$$

алгебры типа AC3, для которых

$$\begin{aligned} e_1 e_2 &= e_1 + e + 2, \\ e_2 e_3 &= e_1 + e_3, \\ e_3 e_1 &= e_2 + e_3; \end{aligned}$$

алгебры типа AC4, для которых

$$\begin{aligned} e_1 e_2 &= \frac{1}{\Delta}(e_1 + p^2 e_2 - p e_3), \\ e_2 e_3 &= \frac{1}{\Delta}((p-1)e_1 + (p-1)^2 e_2 + e_3), \\ e_3 e_1 &= \frac{1}{\Delta}((p-1)^2 e_1 - p(p-1)e_2 + p^2 e_3), \\ \Delta &= p^2 - p + 1, \quad p \neq 0, \quad p \neq 1. \end{aligned}$$

При этом алгебры разных типов не изоморфны между собой. Алгебры типа AC1 с параметрами (a_1, b_1) и (a_2, b_2) изоморфны тогда и только тогда, когда $\{a_2, b_2\} = \{a_1, b_1\}$ или $\{a_2, b_2\} = \{-a_1, -b_1\}$. Алгебры типа AC2 с параметрами (a_1, b_1, c_1) и (a_2, b_2, c_2) изоморфны тогда и только тогда, когда $\{a_2, b_2, c_2\} = \{a_1, b_1, c_1\}$ или $\{a_2, b_2, c_2\} = \{-a_1, -b_1, -c_1\}$. Алгебры типа AC4 с параметрами p_1 и p_2 изоморфны тогда и только тогда, когда $p_1 = p_2$, или $p_1(1-p_2) = 1$, или $(1-p_1)p_2 = 1$.

Доказательство. Покажем вначале, что алгебры типа $AC1$ – $AC4$ являются расширением алгебры комплексных чисел. В алгебре $AC1$ положим $g_1 = e_1 + e_2$, $g_i = ae_1 + be_2 + (a-b)e_3$; в алгебре $AC2$ положим $g_1 = e_1 + e_2 + e_3$, $g_i = ae_1 + be_2 + ce_3$; в алгебре $AC3$ положим $g_1 = e_1 + e_2$, $g_i = (e_1 - e_2 + 2e_3)/\sqrt{3}$; в алгебре $AC4$ положим

$$g_1 = e_1 + e_2, \quad g_i = \frac{2-p}{\sqrt{3p}}e_1 + \frac{1-2p}{\sqrt{3}}e_2 + \frac{p+1}{\sqrt{p-1}}e_3.$$

Во всех случаях можно проверить (в последнем случае довольно громоздко), что $g_1g_1 = g_1$, $g_1g_i = g_ig_1 = g_i$, $g_ig_i = -g_1$, то есть подалгебры, порожденные элементами g_1 и g_i , изоморфны алгебре комплексных чисел.

Пусть теперь AC — произвольная трехмерная алгебра с простым умножением над полем действительных чисел, являющаяся расширением алгебры комплексных чисел, и пусть φ — изоморфное вложение алгебры комплексных чисел в AC . Тогда обозначим $\varphi(1) = g_1$, $\varphi(i) = g_i$. Докажем, что AC изоморфна одной из алгебр $AC1$, $AC2$, $AC3$ или $AC4$. Рассмотрим возможные случаи.

(а) Пусть таблица умножения в AC в базисе e_1, e_2, e_3 имеет вид

$$e_1e_1 = f_1, \quad e_2e_2 = f_2, \quad e_3e_3 = f_3, \quad e_ie_j = 0, i \neq j. \quad (11)$$

Рассмотрим элемент $g_1 = \varphi(1)$. С точностью до перенумерации базисных векторов возможны следующие три подслучая.

(a1) $g_1 = \lambda e_1$, $\lambda_1 \neq 0$. Заменяем в базисе вектор e_1 на λe_1 и новый вектор снова обозначим e_1 . При этом таблица умножения снова будет иметь вид (11) (с другими f_1, f_2, f_3 , вектор f_1 умножится на λ^2 и затем коэффициенты в f_1, f_2, f_3 при e_1 разделятся на λ). Будем считать, что (11) — это таблица умножения в новом базисе. Тогда $g_1 = e_1$ и должно быть $g_1g_1 = g_1$, откуда $f_1 = g_1 = e_1$. Пусть $g_i = ae_1 + be_2 + ce_3$. Тогда должно быть $g_1g_i = g_i$, откуда $g_i = af_1 = ae_1$. Так как φ — изоморфизм, находим, что $i = a$, где a — действительное число, получаем противоречие. Следовательно, случай (a1) невозможен.

(a2) $g_1 = \lambda_1 e_1 + \lambda_2 e_2$, $\lambda_1 \neq 0$, $\lambda_2 \neq 0$. Изменяя масштаб векторов e_1 и e_2 , можно считать, что $g_1 = e_1 + e_2$. Пусть $g_i = ae_1 + be_2 + ce_3$. Тогда должны выполняться тождества $g_1g_1 = g_1$, $g_1g_i = g_i$, $g_ig_i = -g_1$. С учетом (11) получаем систему уравнений

$$f_1 + f_2 = e_1 + e_2, \quad (12)$$

$$af_1 + bf_2 = ae_1 + be_2 + ce_3, \quad (13)$$

$$a^2f_1 + b^2f_2 + c^2f_1 = -e_1 - e_2. \quad (14)$$

Если $c = 0$, то $a \neq b$ (иначе g_i и g_1 коллинеарны). Тогда из (12) и (13) находим, что $f_1 = e_1$, $f_2 = e_2$ и из (14) получаем равенства $a^2 = b^2 = -1$, где a, b — действительные числа, что невозможно. Следовательно $c \neq 0$. Изменяя масштаб e_3 , можно считать, что $c = 1$, то есть $g_i = ae_1 + be_2 + e_3$. В этом случае определитель системы (12)–(14) равен $\Delta = b - a$. Если $a = b$, то из (12) и (13) находим, что $e_3 = 0$, получили противоречие. Следовательно $\Delta = b - a \neq 0$. Тогда f_1, f_2, f_3 определяются из системы (12)–(14). Легко проверить, что решение этой системы при $c = 1$, $a \neq b$, имеет вид

$$f_1 = e_1 - \frac{1}{b-a}e_3, \quad f_2 = e_2 + \frac{1}{b-a}e_3,$$

$$f_3 = -(1 + a^2)e_1 - (1 + b^2)e_2 - (a + b)e_3.$$

Заменим в базисе вектор e_3 на $-e_3/(b - a)$ и новый вектор снова обозначим e_3 . При этом $f_3 = e_3e_3$ умножится на $1/(b - a)^2$ и затем координаты в f_1, f_2, f_3 при e_3 разделятся на $-1/(b - a)$. В новом базисе таблица умножения будет иметь вид $AC1$, то есть в этом случае алгебра AC изоморфна одной из алгебр типа $AC1$.

(а3) $g_1 = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3$, $\lambda_1 \neq 0$, $\lambda_2 \neq 0$, $\lambda_3 \neq 0$. Изменяя масштаб e_1, e_2, e_3 , можем считать, что $g_1 = e_1 + e_2 + e_3$. Пусть $g_i = ae_1 + be_2 + ce_3$. Тождества $g_1g_1 = g_1$, $g_1g_i = g_i$, $g_i g_i = -g_1$ дают следующую систему уравнений:

$$f_1 + f_2 + f_3 = e_1 + e_2 + e_3, \quad (15)$$

$$af_1 + bf_2 + cf_3 = ae_1 + be_2 + ce_3, \quad (16)$$

$$a^2 f_1 + b^2 f_2 + c^2 f_3 = -e_1 - e_2 - e_3. \quad (17)$$

Определитель этой системы равен $\Delta = (a - b)(b - c)(c - a)$. Если $a = b = c$, то g_i и g_1 коллинеарны, что невозможно. Если $b = c \neq a$, то из (15) и (16) находим, что $(a - b)f_1 = (a - b)e_1$ и $f_1 = e_1$. Тогда $f_2 + f_3 = e_2 + e_3$ и из (17) получаем, что $a^2 e_1 + b^2 e_2 + b^2 e_3 = -e_1 - e_2 - e_3$. Отсюда $a^2 = -1$, что невозможно. Следовательно, в силу симметрии получаем, что $a \neq b$, $b \neq c$, $a \neq c$ и $\Delta = (a - b)(b - c)(c - a) \neq 0$. Тогда f_1, f_2, f_3 однозначно определяются из системы (15)–(17). Нетрудно проверить, что решение этой системы имеет вид

$$f_1 = e_1 + \frac{b - c}{\Delta} F, \quad f_2 = e_2 + \frac{c - a}{\Delta} F, \quad f_3 = e_3 + \frac{a - b}{\Delta} F,$$

$$F = (a^2 + 1)e_1 + (b^2 + 1)e_2 + (c^2 + 1)e_3,$$

и, следовательно, в этом случае алгебра AC изоморфна одной из алгебр типа $AC2$.

(b) Пусть таблица умножения в AC в базисе e_1, e_2, e_3 имеет вид $e_1 e_1 = f_1$, $e_2 e_3 = f_2$, $e_3 e_2 = f_3$. Допустим, что AC содержит подалгебру A_1 , изоморфную алгебре комплексных чисел, и g_1, g_i — элементы, соответствующие 1 и i в A_1 . Покажем, что это ведет к противоречию. Пусть $g_1 = a_1 e_1 + b_1 e_2 + c_1 e_3$ и $g_i = a_2 e_1 + b_2 e_2 + c_2 e_3$. Тогда должны выполняться равенства

$$g_1 g_1 = a_1^2 f_1 + b_1 c_1 (f_2 + f_3) = g_1, \quad (18)$$

$$g_1 g_i = a_1 a_2 f_1 + b_1 c_2 f_2 + c_1 b_2 f_3 = g_i, \quad (19)$$

$$g_i g_1 = a_1 a_2 f_1 + b_2 c_1 f_2 + c_2 b_1 f_3 = g_i, \quad (20)$$

$$g_i g_i = a_2^2 f_1 + b_2 c_2 (f_2 + f_3) = -g_1. \quad (21)$$

Вычитая (20) из (19) и складывая (18) и (21), получаем, что

$$(b_1 c_2 - b_2 c_1)(f_2 - f_3) = 0, \quad (22)$$

$$(a_1^2 + a_2^2)f_1 + (b_1 c_1 + b_2 c_2)(f_2 + f_3) = 0. \quad (23)$$

Рассмотрим два подслучая.

(b1) $f_2 = f_3$. Так как g_1 и g_i не коллинеарны, из (18) и (19) следует, что f_1 не коллинеарен f_2 . Тогда из (23) следует, что $a_1^2 + a_2^2 = 0$, то есть $a_1 = a_2 = 0$. Но тогда из (18) и (19) следует, что g_1 и g_i коллинеарны, получили противоречие.

(b2) $f_2 \neq f_3$. Тогда из (22) следует, что $b_1c_2 - b_2c_1 = 0$, то есть векторы $b_1e_2 + c_1e_3$ и $b_2e_2 + c_2e_3$ коллинеарны некоторому одному и тому же ненулевому вектору $be_2 + ce_3$. Так как двумерная алгебра A_1 порождается векторами g_1 и g_i , в данном случае она порождается векторами e_1 и $be_2 + ce_3$. Но $e_1(be_2 + ce_3) = 0$, то есть получаем, что в A_1 есть делители нуля, что невозможно, поскольку в изоморфной ей алгебре комплексных чисел делителей нуля нет.

(с) Пусть таблица умножения в AC в базисе e_1, e_2, e_3 имеет вид $e_1e_2 = f_1$, $e_2e_3 = f_2$, $e_3e_1 = f_3$. С точностью до перенумерации базисных векторов возможны следующие случаи.

(c1) $g_1 = \lambda e_1$. Тогда $g_1 = g_1g_1 = 0$, получаем противоречие.

(c2) $g_1 = \lambda_1 e_1 + \lambda_2 e_2$, $\lambda_1 \neq 0$, $\lambda_2 \neq 0$. Изменяя масштаб e_1 и e_2 , можем считать, что $g_1 = e_1 + e_2$. Пусть $g_i = ae_1 + be_2 + ce_3$. Тогда равенства $g_1g_1 = g_1$ и $g_1g_i = g_ig_1 = g_i$ принимают вид

$$f_1 = e_1 + e_2, \quad (24)$$

$$bf_1 + cf_2 = ae_1 + be_2 + ce_3, \quad (25)$$

$$af_1 + cf_3 = ae_1 + be_2 + ce_3. \quad (26)$$

Если $c = 0$, то $a \neq 0$ или $b \neq 0$ и f_1 коллинеарен g_i . Но $f_1 = g_1$, получили противоречие. Следовательно, $c \neq 0$. Вычитая из (25) и (26) уравнение (24), умноженное, соответственно, на b и на a , получим, что

$$f_2 = \frac{a-b}{c}e_1 + e_3, \quad f_3 = \frac{b-a}{c}e_2 + e_3.$$

Если $b = a$, то $f_2 = f_3 = e_3$ и $g_i = ae_1 + ae_2 + ce_3$. Тогда

$$g_ig_i = a^2f_1 + acf_2 + acf_3 = a^2(e_1 + e_2) + 2ace_3 = -g_1,$$

откуда $a^2 = -1$, получили противоречие. Следовательно, $b \neq a$. Заменяем в базисе вектор e_3 на $ce_3/(a-b)$ и новый вектор снова обозначим e_3 . При этом f_2 и f_3 умножатся на $c/(a-b)$, а затем коэффициенты при e_3 во всех f_j поделятся на $c/(a-b)$. Получим, что $f_1 = e_1 + e_2$, $f_2 = e_1 + e_3$, $f_3 = -e_1 + e_3$. Таким образом, в этом случае алгебра AC может быть изоморфна только алгебре типа $AC3$.

(с3) $e_1e_2 = f_1$, $e_2e_3 = f_2$, $e_3e_1 = f_3$ и $g_1 = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3$, где $\lambda_1 \neq 0$, $\lambda_2 \neq 0$, $\lambda_3 \neq 0$. Изменяя масштаб базисных векторов, можно считать, что $g_1 = e_1 + e_2 + e_3$. Пусть $g_i = ae_1 + be_2 + ce_3$. Тогда $g_i - cg_1 = (a-c)e_1 + (b-c)e_2 \in A_1$, где A_1 — подалгебра в AC , порожденная элементами g_1 и g_i (и, следовательно, изоморфная алгебре комплексных чисел). Если $a = c$, то $(b-c)e_2 \in A_1$, причем $b-c \neq 0$, так как $g_i \neq cg_1$. Тогда $e_2 \in A_1$ и $e_2e_2 = 0$, что невозможно, поскольку в алгебре комплексных чисел нет делителей нуля. Следовательно, $a \neq c$ и в A_1 входит некоторый элемент $e_1 + pe_2$, причем так же, как выше, получаем, что $p \neq 0$. Так как g_1 — единица в подалгебре A_1 , получаем следующую систему уравнений:

$$g_1g_1 = f_1 + f_2 + f_3 = e_1 + e_2 + e + 3,$$

$$g_1(e_1 + pe_2) = pf_1 + f_3 = e_1 + pe_2,$$

$$(e_1 + pe_2)g_1 = f_1 + pf_2 = e_1 + pe_2.$$

Определитель этой системы $\Delta = p^2 - p + 1 \neq 0$ при любом (действительном) p . Нетрудно проверить, что решение этой системы имеет вид

$$\begin{aligned} f_1 &= \frac{1}{\Delta}(e_1 + p^2 e_2 - p e_3), \\ f_2 &= \frac{1}{\Delta}((p-1)e_1 + (p-1)^2 e_2 + e_3), \\ f_3 &= \frac{1}{\Delta}((p-1)^2 e_1 - p(p-1)e_2 + p^2 e_3), \end{aligned}$$

где $\Delta = p^2 - p + 1$ и $p \neq 0$. Допустим, что $p = 1$. Тогда в A_1 содержатся элементы $e_1 + e_2 + e_3$ и $e_1 + e_2$. Следовательно, в A_1 содержится и e_3 . Но $e_3 e_3 = 0$, что невозможно, так как в алгебре комплексных чисел нет делителей нуля. Таким образом, $p \neq 0$ и $p \neq 1$. Получаем, что AC — одна из алгебр типа $AC4$.

Проверим теперь, при каких условиях алгебры типа $AC1$ – $AC4$ изоморфны между собой. Пусть V — некоторая алгебра над полем K и $x \in V$. Положим $xV = \{xa \mid a \in V\}$. Элемент x алгебры V будем называть уникальным, если $\dim xV \leq 1$.

Лемма 4. Пусть V — алгебра с простым умножением с таблицей умножения $e_i e_{\sigma(i)} = f_i$, $i = 1, 2, \dots, n$ и $e_i e_j = 0$ при $j \neq \sigma(i)$. Тогда векторы e_i и коллинеарные им векторы уникальны, а если среди f_i нет коллинеарных векторов, то уникальны только векторы, коллинеарные векторам e_i .

Доказательство. Так как $e_i e_j = 0$ при $j \neq \sigma(i)$, для любого $a \in V$ и любого $\lambda \in K$ вектор $(\lambda e_i)a$ коллинеарен f_i . Следовательно, вектор λe_i уникален. Пусть, с другой стороны, $x = x_1 e_1 + \dots + x_n e_n$ и $x_j \neq 0$, $x_k \neq 0$. Тогда вектор $x e_{\sigma(j)}$ коллинеарен f_j и вектор $x e_{\sigma(k)}$ коллинеарен f_k . Если f_j и f_k не коллинеарны, то $\dim xV \geq 2$ и x не уникален. Лемма доказана.

Пусть V и V' — две алгебры типа $AC1$ – $AC4$ над полем действительных чисел с таблицами умножения $e_i e_{\sigma(i)} = f_i$ и $e'_j e'_{\tau(j)} = f'_j$. Пусть φ — изоморфизм V на V' . Легко видеть, что в каждой таблице умножения для алгебр типа $AC1$ – $AC4$ векторы в правой части не коллинеарны. Следовательно, по лемме 4, в V уникальны только векторы, коллинеарные базисным векторам e_1, e_2, e_3 , а в V' уникальны только векторы, коллинеарные базисным векторам e'_1, e'_2, e'_3 . Так как уникальность сохраняется при изоморфизме, то $\varphi(e_i) = \lambda_i e'_{\rho(i)}$, где $\rho(i)$ — некоторая подстановка на множестве $\{1, 2, 3\}$ и $\lambda_i \in K$, $\lambda_i \neq 0$. Так как в алгебрах типа $AC1$ и $AC2$ $e_i e_i \neq 0$, а алгебрах типа $AC3$ и $AC4$ $e_i e_i = 0$, алгебры типа $AC1$ и $AC2$ не изоморфны алгебрам типа $AC3$ и $AC4$.

Пусть V^2 обозначает линейную оболочку над K множества $\{ab \mid a \in V, b \in V\}$. Тогда V^2 является линейной оболочкой векторов f_1, f_2, f_3 . Нетрудно проверить, что в любой из алгебр типа $AC1$ – $AC4$ $\text{rank}\{f_1, f_2, f_3\} = 2$ (в алгебре $AC2$ выполняется равенство $(1+a^2)f_1 + (1+b^2)f_2 + (1+c^2)f_3 = 0$, а в алгебре $AC4$ координаты x_1, x_2, x_3 каждого вектора f_i удовлетворяют соотношению $px_1 - x_2 + (1-p)x_3 = 0$). Пусть A — подалгебра в V , изоморфная алгебре комплексных чисел. Тогда $A = A^2 \subseteq V^2$. Так как $\dim A = \dim V^2 = 2$, то $V^2 = A$, то есть V^2 и, аналогично, $(V')^2$ изоморфны алгебре комплексных чисел. Пусть g_1, g'_1, g_i, g'_i — элементы в V^2 и $(V')^2$, соответствующие комплексным числам 1 и i . При этом g_1 и g'_1

определяются однозначно, g_i и g'_i определяются с точностью до умножения на -1 . Так как φ — изоморфизм V на V' , то φ — изоморфизм V^2 на $(V')^2$. Поэтому $\varphi(g_1) = g'_1$ и $\varphi(g_i) = g'_i$ или $\varphi(g_i) = -g'_i$.

Пусть V — алгебра типа $AC1$ или $AC3$. Тогда (см. выше) $g_1 = e_1 + e_2$ и $\varphi(g_1) = \lambda_1 e'_{\rho(1)} + \lambda_2 e'_{\rho(2)} = g'_1$. Следовательно, алгебры типа $AC1$ и $AC3$ не изоморфны алгебрам типа $AC2$ и $AC4$. Таким образом, алгебры различных типов не изоморфны между собой.

Пусть V и V' — алгебры типа $AC1$ с параметрами $\{a, b\}$ и $\{a', b'\}$. Так как $g_1 = e_1 + e_2$, $g'_1 = e'_1 + e'_2$ и $\varphi(g_1) = \lambda_1 e'_{\rho(1)} + \lambda_2 e'_{\rho(2)} = g'_1$, то $\rho(\{1, 2\}) = \{1, 2\}$, $\rho(3) = 3$ и $\lambda_1 = \lambda_2 = 1$. Можно взять (см. выше) $g_i = ae_1 + be_2 + (a - b)e_3$ и $g'_i = a'e'_1 + b'e'_2 + (a' - b')e'_3$. При этом $\varphi(g_i) = g'_i$ или $\varphi(g_i) = -g'_i$. Так как $\varphi(\{e_1, e_2\}) = \{e'_1, e'_2\}$, то $(a', b') = \pm(a, b)$ или $(a', b') = \pm(b, a)$. Легко видеть, что в первом случае действительно есть изоморфизм V на V' , а именно, $\varphi(e_1) = e'_1$, $\varphi(e_2) = e'_2$, $\varphi(e_3) = e'_3$. Во втором случае также есть изоморфизм $\varphi(e_1) = e'_2$, $\varphi(e_2) = e'_1$, $\varphi(e_3) = -e'_3$.

Пусть V и V' — алгебры типа $AC2$ с параметрами $\{a, b, c\}$ и $\{a', b', c'\}$. Тогда $g_1 = e_1 + e_2 + e_3$, $g'_1 = e'_1 + e'_2 + e'_3$. Следовательно, $\varphi(\{e_1, e_2, e_3\}) = \{e'_1, e'_2, e'_3\}$. Можно взять $g_i = ae_1 + be_2 + ce_3$ и $g'_i = a'e'_1 + b'e'_2 + c'e'_3$. Тогда $\varphi(g_i) = g'_i$ или $\varphi(g_i) = -g'_i$. Поэтому $\{a', b', c'\} = \{a, b, c\}$ или $\{a', b', c'\} = \{-a, -b, -c\}$. Нетрудно видеть, что при таких условиях действительно существует изоморфизм V на V' , а именно, $\varphi(e_j) = e'_{\rho(j)}$ для некоторой подстановки ρ .

Пусть V и V' — алгебры типа $AC4$ с параметрами p и p' . Тогда $g_1 = e_1 + e_2 + e_3$, $g'_1 = e'_1 + e'_2 + e'_3$. Следовательно, $\varphi(\{e_1, e_2, e_3\}) = \{e'_1, e'_2, e'_3\}$, причем $\varphi(e_j) = e'_{\rho(j)}$, где ρ — либо тождественная, либо циклическая подстановка на множестве $\{1, 2, 3\}$. В алгебре $AC4$ координаты x_1, x_2, x_3 всех векторов f_1, f_2, f_3 , стоящих в правых частях в таблице умножения, удовлетворяют соотношению $px_1 - x_2 + (1-p)x_3 = 0$, и $\text{rank}\{f_1, f_2, f_3\} = 2$. Поэтому $e_1 + pe_2 \in V^2$. Тогда $\varphi(e_1 + pe_2) \in (V')^2$ и $\varphi(e_1 + pe_2) = e'_1 + pe'_2$, либо $\varphi(e_1 + pe_2) = e'_2 + pe'_1$, либо $\varphi(e_1 + pe_2) = e'_3 + pe'_1$. Но координаты y_1, y_2, y_3 любых векторов в $(V')^2$ удовлетворяют соотношению $p'y_1 - y_2 + (1-p')y_3 = 0$. Поэтому либо $p' - p = 0$, либо $-1 + p(1 - p') = 0$, либо $pp' + (1 - p') = 0$, то есть либо $p' = p$, либо $p(1 - p') = 1$, либо $p'(1 - p) = 1$. Можно проверить, что при $p(1 - p') = 1$ отображение φ такое, что $\varphi(e_1) = e'_2$, $\varphi(e_2) = e'_3$, $\varphi(e_3) = e'_1$ — действительно изоморфизм V на V' , а при $p'(1 - p) = 1$ изоморфизмом V на V' является отображение φ такое, что $\varphi(e_1) = e'_3$, $\varphi(e_2) = e'_1$, $\varphi(e_3) = e'_2$.

Теорема 2 полностью доказана.

Список литературы

1. Алексеев В. Б. Сложность умножения матриц. Обзор. *Киберн. сб.* (1988) **25**, 189–236.
2. de Groote H. F. On varieties of optimal algorithms for the computation of bilinear mappings II. Optimal algorithms for 2×2 matrix multiplication. *Theoretical Comput. Sci.* (1978) **7**, №2, 127–148.

Статья поступила 16.05.94.